我國刑法電腦犯罪修正條文之立法比較及實務問題研究

作者：葉奇鑫[1]

壹、 前言

為因應高科技時代層出不窮之電腦犯罪案例，我國刑法曾於民國八十六年十月八日公布修正及增訂共計九個條文（以下簡稱：八十六年電腦犯罪條文）[2]，該次修法及時解決了當時司法界處理電腦犯罪案例時，法律適用上之困境，對於近五年來電腦犯罪查緝實務之發展，確實有重大貢獻。惟近年來因網路快速發展，電腦犯罪手法不斷翻新，為有效規範新型態之電腦犯罪，並使我國電腦犯罪之法律規範能符合世界先進國家之標準[3]，法務部於九十年五月邀集產官學界代表共同組成「法務部防制電腦（網路）犯罪相關法規研究小組」（以下簡稱電腦犯罪法規研究小組），歷經一年多之理性辯論，逐步將共識形成具體草案文字[4]。該草案經行政院審查後會銜司法院送立法院審議，立法院於九十二年六月三日三讀通過本草案[5]， 總統並於九十二年六月二十五日公布。至此，我國刑法新增第三十六章「妨害電

---

[1] 本文作者為交通大學電子工程系畢業，東吳大學法律研究所碩士，現職法務部檢察司調辦事檢察官，電子信箱：simon061@ms3.hinet.net

[2] 修正條文計有四條：刑法第二百二十條、第三百一十五條、第三百二十三條、第三百五十二條。增訂條文則有五條，分別為：第三百一十八條之一及之二、第三百三十九條之一至之三。

[3] 法務部於本次修法之初，即確立以歐洲網路犯罪公約為本次立法之重要參考方向，參見電腦犯罪法規研究小組九十年十二月二十七日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第八十六至八十七頁。另關於歐洲網路犯罪公約與我國相關法律（實體法部分）比較表，亦請參見上開彙編第三百一十三至三百二十頁。

[4] 關於法務部防制電腦（網路）犯罪相關法規研究小組前後共十一次會議之完整會議記錄、各草案版本及外國參考資料等，均收錄於「刑法有關電腦（網路）犯罪研修資料彙編」，九十二年十二月，法務部印製。

[5] 修正條文及立法理由之電子檔，可於「立法院全球資訊網」（網址：http://www.ly.gov.tw/ly/index.jsp）之「法律資料庫」檢索，或於法務部部內網站首頁下載。

腦使用罪」章（簡稱電腦犯罪專章），專以處理狹義之電腦犯罪[6]。

筆者因職務關係有幸全程參與修法過程，且鑒於新修正電腦犯罪條文將對我國實務審理電腦犯罪案件之法律適用將產生重大影響，因此不惴學識淺陋，為文將修法重點與各方先進共享，除期發揮拋磚引玉之效果外，並願藉此文對所有參與本法案之先進表達由衷之感謝。

貳、 我國電腦犯罪實體法之體系與架構

傳統刑法於訂定搶奪、強盜、竊盜等諸多財產犯罪行為態樣及刑度時，係以有體物之保護為思考基礎，進而以不法腕力之有無，及其他可能造成人身危險之因素（例如：夜間、攜帶凶器、結夥人數等）來區分罪名與刑度，此與電腦網路犯罪決勝於千里之外之無形犯罪特質，本質上有極大之不同，故世界各先進國家均以獨立之電腦犯罪條文規範電腦犯罪行為。我國八十六年電腦犯罪條文基本上仍係架構於傳統刑法之基礎上發展，除創設電磁紀錄之概念且將準文書之範圍擴張至電磁紀錄外（刑法第二百二十條），並將電磁紀錄擬制為動產（原刑法第三百二十三條），使電磁紀錄得以藉傳統刑法之竊盜罪、侵占罪（刑法第三百三十八條準用）、詐欺罪（刑法第三百四十三條準用）、搶奪及強盜罪（刑法第三百三十四條之一準用）獲得保護。本次修法則因考量電腦已成為日常生活之重要工具，電腦使用安全、電磁紀錄支配權及電腦系統效能等應已成為值得獨立保護之法益，因此設立專章獨立保護上開法益，又由於電腦安全等法益於新法中已受到充分保護，因此本次修法同時刪除八十六年電腦犯罪條文中將電磁紀錄擬制為動產之規定，以避免發生法條競合之情形，並進而將法律問題簡

[6] 一般而言，廣義之電腦犯罪係指以電腦為工具犯傳統型犯罪，例如：網路詐欺、網路色情等。而狹義電腦犯罪則指以電腦或網路為攻擊標的之犯罪，例如：駭客入侵、電腦病毒等

化，以受攻擊客體係有體物或無體物為區分標準，如為有體物（例如：搶奪磁片或竊取電腦），則以傳統刑法評價，如為無體物（如駭客入侵網站並竊取電磁紀錄），則以電腦犯罪專章處理。以下謹逐條說明新增之刑法第三十六章妨害電腦使用罪章。

參、 妨害電腦使用罪章逐條釋義與問題探討

一、章名：妨害電腦使用罪

如前所述，本章係以狹義電腦犯罪，亦即以電腦或網路為攻擊標的之行為作為規範對象。本章章名原擬為「電腦犯罪」，惟從立法技術之角度來看，刑法章名向以「某某罪」為名，例如：殺人罪、傷害罪或竊盜罪等，並未有「某某犯罪」之章名體例，因此於草案研擬過程中又仿英國Computer Misuse Act，將章名改為「濫用電腦罪」[7]。惟學者認為：「濫用」一詞係指有權使用者超越正當合理使用之情形，與本章目的係保障他人電腦使用之不受侵害不符[8]。故最後以甘添貴及靳宗力教獸所提議之「妨害電腦使用罪」為章名[9]。

另，有學者主張電腦一詞似不足以涵蓋網際網路空間之部分[10]。更有專家認為：網路為電腦連結而成，網路犯罪為電腦犯罪之一種類型，電腦犯罪與網路犯罪之定義與範圍有所不同[11]。上開對電腦犯罪及網路犯罪之區分，固非無見。惟如從外國之經驗來看，所謂電腦犯罪(Computer Crime)與網路犯罪(Cybercrime)之區隔，卻非如此絕對。

---

[7] 參見電腦犯罪法規研究小組九十一年三月一日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第一百三十一頁。

[8] 參見電腦犯罪法規研究小組九十一年五月二十日會議記錄，靳宗立教授之發言，「刑法有關電腦（網路）犯罪研修資料彙編」，第二百三十一頁。

[9] 同前揭註，第二百三十頁至第二百三十三頁。

[10] 同前揭註，第二百三十頁。

[11] 參見吳芙如檢察官著，「網路犯罪之管轄權」，收錄於 2003 網路犯罪與智權保護研討會論文集，第二十一至第二十二頁。

據美國學者於二００一年二月十日，分別從Westlaw及Findlaw法律資料庫搜尋之結果，均顯示美國法院判決並未使用Cybercrime一字，惟於Westlaw中則可查得九十四個使用Computer Crime一詞之法院判決[12]。又美國最重要之網路犯罪政策單位：美國司法部「電腦犯罪與智慧財產權處」（CCIPs）之全稱為"Computer Crime" and Intellectual Property Section，並非使用Cyber Crime。但歐洲網路犯罪公約（Convention on Cybercrime）則使用Cybercrime一詞為名，新近諸多國際會議亦經常使用Cybercrime一詞[13]。由此可見，Computer Crime與Cybercrime之涵義其實並無明顯之差別。況本法保護之客體並不限於網路上之電腦，亦包含單機電腦，因此本章雖未使用「網路」，而係以「電腦」為名，應無不妥。

二、無故入侵他人電腦（刑法第三百五十八條）

刑法第三百五十八條規定：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」本條保護法益係電腦之使用安全，如使用人能合理期待其電腦具有高度之安全性，而該安全性卻因為他人之無故入侵行為而遭受破壞，行為人即可能該當本罪。使用人能合理期待其電腦具有高度安全性之情形可概分為二：

（一）設有保護措施：使用人已為其電腦設有密碼（例如：一般個人電腦系統均具備之 BIOS 密碼、作業系統密碼或螢幕保護程式密碼等），或已安裝其他類似之保護措施（例如：在高階筆記型電腦或 PDA

[12] *See* Ralph D. Clifford, Cybercrime-The Investigation, Prosecution and Defense of a Computer-Related Crime, page 1. (2001)

[13] 例如：APEC今年七月二十一日至二十五日於泰國曼谷舉辦之「亞太經濟合作網路犯罪立法及執法能力建構會議」（Cybercrime Legislation and Enforcement Capacity Building）。香港大學近年定期舉辦之網路犯罪高峰會（Cybercrime

可見到的指紋或聲紋開機辨識系統等），上開密碼及保護措施原足以阻絕他人無故使用電腦，以確保電腦之安全性，但卻因為行為人以盜取之密碼或破解保護措施之方法入侵，此行為縱使未生實質損害（例如：行為人只把玩電腦一會兒即自行離去），該電腦之安全性亦已受到破壞與挑戰，行為人已該當本條之罪。

（二）系統漏洞：使用人原能合理期待電腦係處於安全狀態（最常見之情形為網路上之電腦），但卻因為他人無故利用系統之漏洞而遭到入侵，此種情形雖然使用人未設有保護措施，但因為在正常使用情形下，他人應該無法進入並使用其電腦，使用人因此得以合理期待電腦之安全性，如因行為人利用系統漏洞而遭到入侵，行為人亦可能該當本罪。

由上述分析可知，本條適用之關鍵在於使用人對其電腦安全性是否能有合理之期待，故如電腦未設有密碼，或雖設有密碼，但使用人輸入密碼開機後因故離開時，卻未再設密碼保護，因而遭到他人輕而易舉地不必使用任何密碼或破解手法即得以無故使用其電腦，此類情形原則上均不成立本罪。

又本條所稱之保護措施，與著作權法本次修正草案所列之科技保護措施（Technological Protection Measures ）[14]概念並不相同，最主要之差別在於保護之目的與對象不同，前者為限制電腦之使用，後者則為限制著作之利用，所以如果在自己所有之電腦上安裝某廠牌軟體時，利用破解軟體規避輸入註冊碼之科技保護措施，此行為人可能違反著作權法，但卻不構成本罪，因為該電腦乃行為人所有，行為人並沒有破壞任何人之電腦安全。惟因本次著作權法修正草案於九十二年

Summit）等，均使用Cybercrime一詞。

[14] 智慧財產局本次提出之著作權法修正草案中關於科技保護措施之定義與規定，文字大致上與美國著作權法 17 U.S.C. §1201 規定相同。

六月五日立法院朝野協商時，科技保護措施之條文已被刪除[15]，因此今年六月六日三讀通過之著作權法並未將科技保護措施納入規範，法律適用上暫時沒有混淆之虞。

二、無故取得、變更、刪除電磁紀錄（第三百五十九條）

刑法第三百五十九條規定：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」本條保護之法益為電磁紀錄之支配權。由於本條已將電磁紀錄直接列為保護之對象，因此於電磁紀錄被無故刪除之情形，不須再考慮電磁紀錄是否符合文義性而符合「準文書」之要件。又此次修法已將電磁紀錄擬制為動產之規定刪除（刑法第三百二十三條），故於無故取得他人電磁紀錄之情形，亦無須考慮傳統竊盜罪之「破壞他人持有並進而建立自己持有」之構成要件，法律適用上均較為單純。實務上目前常見之虛擬寶物竊盜案件，未來亦將不再論以竊盜罪，而改論以本罪。

三、無故干擾他人電腦（第三百六十條）

刑法第三百六十條規定：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」本條保護之法益為電腦系統之效能。本條精神上與原刑法第三百五十二條第二項「干擾他人電磁紀錄罪」相近，本次修正之目的在於釐清干擾之方式限於電腦程式或其他電磁方式[16]，又原刑法第三百五十二條第二項保護之對象為

[15] 筆者因職務關係，亦全程見證著作權法草案朝野協商過程。立法委員於朝野協商時刪除著作權法草案中關於科技保護措施之相關條文，其主要理由即為：著作權法草案之科技保護措施，於刑法第三百八十五條中已經規定，勿庸再予重複規定。筆者認為：科技保護措施立法與否，當屬可供社會公評事項，惟如以刑法第三百五十八條已有重複規定為由，而刪除該草案科技保護措施之條文，則為對於刑法第三百五十八條之誤解。

[16] 原刑法第三百五十二條第二項干擾電磁紀錄罪，並未將攻擊方式明確界定，造

「電磁紀錄之處理」，新法則改為「電腦或其相關設備」。本條文適用上之關鍵在於判斷行為人之干擾行為是否已「致生損害於公眾或他人」，故常見之垃圾郵件、掃描通訊埠等行為，因尚未「致生損害」[17]，原則上均未構成本罪。又法院目前審理虛擬寶物竊盜案例所適用之法條，見解並不統一，有法官除認為除構成竊盜罪與詐欺得利罪外，尚構成原刑法之干擾電磁紀錄罪，此見解於現行法固非無據，惟於新法公布施行後，此見解恐須變更，因為輸入他人帳號密碼進而移轉竊取虛擬寶物，均為原遊戲平台提供之功能，此種行為嚴格說來並未影響系統之效能，所發生之損害乃係因伺服器之電磁紀錄被變更所致，而此部份已有前述之刑法第三百五十九條可資規範。至於極具爭議性之遊戲外掛程式，是否該當本條？亦應視其是否「致生損害」而定，以練功程式為例，如果該程式係以正常遊戲節奏自動操作角色進行練功或尋寶，此種程式並未影響到系統效能，應不該當本罪，反之，如果該程式係以非常誇張之密集封包傳送方法「加速」練功，此種程式會造成伺服器超過負荷而當機，因而致生損害，如行為人主觀上亦對此種損害之發生有所預見，則可能（並非一定）該當本罪。至於影響系統效能到什麼程度方能認為是致生損害，很難量化，必須透過實務逐步累積案例。

四、公務機關電腦之加重規定（第三百六十一條）

刑法第三百六十一條規定：「對於公務機關之電腦或其相關設備

成文義射程太廣，例如：毀損鍵盤、螢幕等毀損硬體之方法，可能干擾電磁紀錄之處理，拔除排線接頭雖未毀損硬體，亦可能干擾電磁紀錄之處理，實則上開例子均屬對有體物之攻擊行為，應以傳統刑法之毀損罪評價即已足。以上例子均請參見甘添貴教授著，體系刑法各論，第二卷，第四百九十二頁，二０００年四月初版。

[17] 關於掃描通訊埠之行為，美國地方法院曾以並未造成損害為由判決無罪。Scott Moulton and Network Installation Computer Services, Inc. v. VC3 (N.D. Ga. November 6, 2000)。

犯前三條之罪者，加重其刑至二分之一。」本條係為加強保護公務機關電腦所設之加重規定，字義上並不難解，有疑問者為告訴乃論與否之問題。本條之立法方式十分類似傷害直系血親尊親屬罪（刑法第二百七十七條、第二百八十條），雖然第二百八十七條並未規定傷害直系血親尊親屬罪是否須告訴乃論，但我國實務向來見解認為：傷害直系血親尊親屬罪性質上為傷害罪之刑度加重，因此仍屬告訴乃論[18]。惟本條之立法原意，原本即欲將之列為非告訴乃論罪，於立法院司法委員會一讀審查時，立法委員亦曾就此罪是否宜採告訴乃論進行詢答，後結論同意採非告訴乃論，故審查會之審查報告中亦補充本條之修正理由略謂：「至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法」。由於立法意旨已明示於立法理由，本條自應解為非告訴乃論之罪，而不應援引實務上對刑法第二百八十條之解釋認第三百六十一條為告訴乃論。

五、製作惡意電腦病毒程式（第三百六十二條）

刑法第三百六十二條規定：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」本條係處罰製作「專供犯本章之罪」之惡意程式之行為，由於構成要件已將該類程式限定於「專供犯本章之罪」之電腦程式（典型之例為：電腦病毒程式及後門程式），且本條文尚以實害之發生為要件，故本條文適用情形著實相當有限，以台灣近六、七年來所查獲之電腦犯罪案例觀察，只有極少數個案（例如：車諾比病毒案件）符合本條之構成要件而已，由於本條在構成要件上相當嚴格，應不至於對軟體產業或學術研究產生影

[18] 參照十九年上字第一九六二號判例要旨。

響。

六、告訴乃論（第三百六十三條）

刑法第三百六十三條規定：「第三百五十八條至第三百六十條之罪，須告訴乃論。」由於科技法律向具爭議性，特別是網際網路源於崇尚學術自由之大學及研究中心，因此「網路公民」向以自由、共享為標榜，甚至有人主張網路空間係一獨立之虛擬新社會，應免於國家統治[19]。故以刑罰約制電腦及網路犯罪之界限應如何拿捏，亦成為本次修法過程中辯論最多之焦點。為避免國家司法權過度介入網路虛擬空間，且為使有限之司法資源能集中於偵辦重大網路犯罪，故本章之罪除第三百六十一條及第三百六十二條之外，其餘之罪均採告訴乃論。

肆、以國際標準檢視本次修法

一、歐洲網路犯罪公約

由於世界各國皆意識到網路犯罪問題之嚴重性，因此國際間乃在歐洲執委會率先倡議，與歐洲議會之主導下，在二００一年十一月二十三日在布達佩斯通過第一個國際性網路犯罪公約[20]。歐洲網路犯罪公約簽署國計有美國、日本、加拿大、南非四個非歐洲議會成員國，及歐洲議會成員中之三十三個國家，而其中已經批准生效者僅有阿爾巴尼亞、克羅埃西亞和愛沙尼亞等三個國家[21]，但誠如美國司法部CCIPs處長瑪莎女士（Martha Stansell-Gamm）於「亞太經濟合作網路

[19] 關於網路法律之探討，請參考劉靜怡教授譯，「網路自由與法律」，Lawrence Lessig，商周出版，二００二年七月二十九日初版。

[20] 關於網路犯罪公約，請參閱馮震宇教授著，「網路犯罪與網路犯罪公約（上）（下）」，月旦法學教室第四期第一百二十四頁至第一百三十六頁、第五期第一百一十五頁至第一百二十四頁，二００三年四月、五月。

[21] 參見Convention on Cybercrime / Chart of signatures and ratifications，http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm (latest visited Oct. 14,

犯罪立法及執法能力建構會議」中演講時指出：歐洲網路犯罪公約應為世界各國網路犯罪立法之下限，而非上限（It's a floor, not a ceiling）[22]。故歐洲網路犯罪公約實已經成為國際間審核各國電腦犯罪相關立法之標準，我國本次電腦犯罪專章之修法亦應以歐洲網路犯罪公約加以檢驗，以符合國際網路犯罪之立法趨勢。

二、APEC 電腦犯罪立法調查

爲瞭解APEC各經濟體電腦犯罪之立法情形，APEC於二００二年底對各經濟體發出問卷調查(SURVEY OF CYBERCRIME LEGISLATION)[23]。該份問卷係以歐洲電腦犯罪公約為範本，共列出三十一項問題，其中與實體法有關者共有十一項，而與狹義電腦犯罪有關者則有下列五項[24]，美國CCIPs並彙整分析各經濟體之立法情形

2003)。

[22] 該會議係於二００三年七月二十一至二十五日於泰國曼谷舉辦，該會議共分成三大主題，第一主題（Session #1）即為「打擊網路犯罪之法律架構」（Legal Frameworks For Combating Cybercrime）。第一主題共分成二日討論（七月二十二日及二十三日），筆者受邀於七月二十二日下午擔任Speaker，介紹我國網路犯罪之立法進度，刑事警察局偵九隊李相臣隊長則受邀於七月二十三日上午擔任Speaker，介紹我國網路犯罪之查緝情形。該次會議之內容請參見「亞太經濟合作網路犯罪立法及執法能力建構會議」出國報告，報告人：戚雅先、盧玲朱、葉奇鑫、李相臣。

[23] 我國之問卷係由電信總局轉法務部檢察司，再由筆者與慶啟人檢察官共同填寫。問卷內容請參閱：
http://www.apjii.or.id/apec/Country%20Surveys/ChinaSurvey.htm (latest visited Oct.14, 2003)

[24] 其他六項屬廣義電腦犯罪者分別為：（六）Offences relating to Computer related forgery (such as the alteration or deletion of computer data with the intent that it be acted on for legal purposes as if it were authentic)、（七）Offences relating to computer related fraud (such as by dishonestly attempting to gain money or property by altering computer data)、（八） Offences relating to the creation, possession, or distribution of child pornography、（九）Offences related to infringements of copyright and related intellectual property rights、（十）Attempt and aiding or abetting in respect of the above computer related offences（十一）Corporate liability in respect of the above computer related offences 。參見前揭註網址

如下[25]：

（一）非法接觸電腦罪（Offences relating to illegal access to a computer）

１、本項目之依據為歐洲電腦犯罪公約第二條，我國現行刑法中與之對應者為第三百五十八條。

２、問卷說明：本項目係指禁止單純之未經授權入侵電腦之行為，例如：電腦駭客等。

３、美方分析意見：全部經濟體均有某種程度之立法，以規範此種犯罪。但某些經濟體在規範時仍有範圍限制，例如：只限於接觸電腦程式或資料時才犯罪，或者必須規避某種限制接觸之保護功能才犯罪。

４、本文分析意見：我國刑法第三百五十八條即屬美方所指「規範時仍有範圍限制，例如：必須規避某種限制接觸之保護功能才犯罪」之情形，惟此部分其實是我國立法政策選擇後之結果，於草擬條文時即經過充分討論，當時與會專家學者多認為：如果未經授權或無故使用他人電腦即構成本罪，處罰範圍可能太廣，對社會將造成衝擊，因此刻意將電腦之範圍限定在已經設有保護措施之電腦，或雖未設有保護措施，但正常使用情形並不會被入侵之電腦[26]。

（二）非法擷取電子通訊罪（Offences relating to illegal interception of electronic communications）

１、本項目之依據為歐洲電腦犯罪公約第三條，我國現行刑法中與之對應者為第三百五十九條，另如果擷取之電子資料

[25] 以下美方分析意見部分，均請參見「亞太經濟合作網路犯罪立法及執法能力建構會議」出國報告第九至第十頁。

[26] 參見電腦犯罪法規研究小組九十一年三月二十二日會議記錄，「刑法有關電腦

涉及通訊內容，尚可能涉及通訊保障及監察法。

２、問卷說明：本項係禁止非法之網路監聽。

３、美方分析意見：許多經濟體並未特別針對電子通訊監聽立法，電子通訊之監聽是否等同於電話監聽，而受一般電話監聽法律之規範？美國特別對此提出質疑。

４、本文分析意見：查我國刑法第三百五十九條中之「無故取得」，於解釋上應當包含以有線或無線方式擷取電磁紀錄；又我國實務上向認通訊保障及監察法包含網路監聽，而違法監聽者，依該法第二十四條規定，可處五年以下有期徒刑。故我國雖未直接針對電子通訊監聽立法，仍應認無此項漏洞。

（三）干擾電腦資料罪（Offences relating to interference with computer data）

１、本項目之依據為歐洲電腦犯罪公約第四條，我國現行刑法中與之對應者為第三百五十九條。

２、問卷說明：本項目係指禁止未經授權干擾電腦資料或電腦程式，例如：損害資料正確性、刪除資料、使合法使用者無法使用電腦資料等行為。

３、美方分析意見：大部分經濟體均訂有某種程度之干擾罪，且大部分經濟體並不將非法使用列為本罪之要件，這是好現象。

４、本文分析意見：我國刑法第三百五十九條雖未使用干擾一詞，惟對於電腦資料（我國法稱電磁紀錄）之保護範圍大致相同，故應符合本項標準。

（四）干擾電腦系統罪（Offences relating to Interference with a

（網路）犯罪研修資料彙編」，第一百六十五至第一百七十二頁。

computer system）

１、本項目之依據為歐洲電腦犯罪公約第五條，我國現行刑法中與之對應者為第三百六十條。

２、問卷說明：本項目禁止未經授權干擾電腦系統，例如：關閉電腦系統、妨礙電腦系統正常運作、使合法使用者無法使用電腦系統等行為。

３、美方分析意見：許多經濟體有立法規範干擾電腦系統罪，但有部分經濟體只處罰干擾電腦資料之行為，而未特別規範針對電腦系統之干擾行為。

４、本文分析意見：查我國刑法第三百六十條即係以電腦或其相關設備為保護客體，並無美方所指之情形，應符合本項標準。

（五）濫用裝置罪（Offences relating to misuse of devices）

１、本項目之依據為歐洲電腦犯罪公約第六條，我國現行刑法中與之對應者為第三百六十二條。

２、問卷說明：本項目係禁止生產、散布、販售或持有可以犯上開罪之裝置，例如：帳號密碼、可用以入侵之軟體工具及非法監聽程式（Sniffers）等。

３、美方分析意見：許多經濟體並未特別針對生產、散布、販售或持有可以犯上開罪之「裝置」立法處罰，部分經濟體僅處罰移轉（transfer）使用裝置（access devices）之行為。

４、本文分析意見：查我國刑法第三百六十二條僅處罰製作專供犯本章之罪之電腦程式，就行為而言，並未規範到散布、販售及持有等行為，就工具種類而言，我國法僅限於電腦程式，並不包括帳號密碼等，範圍確實較歐洲網路犯罪公約要

求之標準狹窄許多。然本項目之立法其實仍具爭議性，世界各國軟體業者對本項目之立法亦多所疑慮，本法規範範圍雖然遠較歐洲網路犯罪公約之要求狹窄，但於草擬過程中，仍有委員強烈反對刑法第三百六十二條，認為本條會對國內軟體產業及學術研究造成不利之影響[27]。甚至美國CCIPs處長瑪莎女士於泰國會議中亦坦言：「美方亦花了許多時間精力與軟體產業溝通，以解除軟體業界對此立法之疑慮。」又歐洲網路犯罪公約第六條第三項亦規定：電腦密碼、使用碼（access code）或類此資料之部分，簽署國可保留不立法，可見關於帳號密碼之部分更具高度爭議性。故我國未來就裝置濫用部分如欲全面採取歐洲網路犯罪公約之標準，必須廣納雅言，事先與軟體產業及學術研究單位充分溝通，以避免反彈與誤解。

三、小結

本次電腦犯罪專章修法雖仍未完全符合歐洲電腦犯罪公約之要求，但較之修法前，已有相當大之進步，在 APEC 經濟體中，亦已屬先進之實體法。我國接下來應重新檢視並修法者，應為網路犯罪程序法之部分，惟因程序法部分已超越本文所探討之範疇，擬另文論述之。

伍、虛擬寶物竊盜案件之新舊法比較問題

在本次刑法修正前，雖然有少數意見認為不應以刑法處罰虛擬寶物之竊盜行為[28]，惟法院實務上幾乎均肯認虛擬寶物為電磁紀錄，而

[27] 參見電腦犯罪法規研究小組九十一年四月三日會議記錄，「刑法有關電腦（網路）犯罪研修資料彙編」，第一百九十至第一百九十七頁。

[28] 是否應以竊盜罪處罰目前實務常見之虛擬寶物竊盜行為，實務界曾有不同價值觀之精采辯論，內容詳見：九十二年二月二十一日法務部法檢字第０九二０八００六九六號函。該函可於「法源法學資料檢索系統單機版/刑法/第三百二十條/

依刑法第三百二十三條將電磁紀錄擬制為動產之規定，虛擬寶物之竊盜已構成刑法第三百二十三條、第三百二十條之竊取他人電磁紀錄罪。由於本次刑法修正已將刑法第三百二十三條中電磁紀錄擬制為動產之規定予以刪除，故竊取他人虛擬寶物之行為，於刑法修正後即無法再適用竊盜罪處罰，而必須改以刑法第三百五十八條、第三百五十九條之規定處罰[29]。

比較有疑問者，乃虛擬寶物竊盜之行為時點係於刑法修正前，而裁判時點卻於刑法修正後之情形，此情形涉及新舊法之比較問題，且筆者觀察新近實務判決，對於此種犯罪行為之新舊法比較，似有不同見解，有認為比較新舊法之結果，因新法將此種犯罪改列為告訴乃論之罪，故以新法較為有利於行為人，適用新法判決[30]。亦有認為因新法第三百五十九條所定之罰金刑（二十萬元）高於刑法第三百二十條之罰金刑（五百元），比較新舊法之結果，應以舊法較有利於行為人，而適用舊法判決[31]。

關於行為後刑罰法律有變更時，究應如何適用法律，我國刑法係採「從新從輕之原則」，亦即原則上適用裁判時之新法，但裁判前之舊法有利於行為人時，例外適用裁判前之舊法[32]。至於裁判時之新法與裁判前之舊法何者較為有利之比較，應依照刑法第三十五條之規定：「主刑之重輕，依第三十三條規定之次序定之。同種之刑，以最

法律問題」中檢索查閱。

[29] 一般而言，竊取虛擬寶物之行為可分為三階段，第一階段為取得被害人之帳號密碼，第二階段為登入遊戲伺服器，輸入被害人之帳號密碼，第三階段則為操作被害人帳號中之角色，並將該角色中之虛擬寶物移轉給自己或第三人之角色。第二階段於修法前並無法可罰，第三階段實務通說則以竊盜罪處罰。修法後，第二階段可能觸犯刑法第三百五十八條，第三階段則可能觸犯刑法第三百五十九條。

[30] 參見臺灣板橋地方法院九十二年度易字第一八八八號刑事判決。

[31] 參見臺灣高等法院九十二年度上易字第一二一二號刑事判決。

[32] 刑法第二條第一項規定：「行為後法律有變更者，適用裁判時之法律。但裁判前之法律有利於行為人者，適用最有利於行為人之法律。」

高度之較長或較多者為重。但最高度相同者，以最低度之較長或較多者為重。除前二項規定外，刑之重輕參酌前二項標準定之。不能依前二項標準定之者，依犯罪情節定之。」依上開規定觀之，舊法似較有利於行為人。

惟如行為後法律之訴追條件（告訴乃論與否）有所變更[33]，則此是否屬於刑法法律之變更而有新舊法比較之問題？又應如何加以比較？臺灣高等法院研究意見認為：告訴權之行使、撤回固屬國家刑罰權得否發動，即刑事訴訟之訴追條件具備與否之刑事程序問題，雖程序應從新，惟某種行為應否劃歸屬告訴乃論之罪，因事涉國家刑罰權得否據以發動所依憑之內容及其範圍之界定，乃具實體性質，就此層面而言，對某種犯罪行為是否得以發動國家刑罰權予以制裁，恒宥於該類型化之犯罪是否屬告訴乃論之罪，並受制於告訴權人是否行使告訴權或撤回告訴，準此，告訴權之行使、撤回與否，並非得以單純之程序問題視之。此因事涉國家刑罰權其內容及範圍之劃定，仍應認係法律有變更，而有比較新舊法之適用。又新舊法比較之結果，以對國家刑罰之發動所做一定限制之規定，較有利於行為人，亦即以劃定為告訴乃論之罪之規定為較有利於行為人[34]。上開研究意見顯認為：行為後法律之訴追要件有所變更，仍有新舊法比較之適用，且以告訴乃論規定之法律為較有利於行為人。由此觀之，新法反較有利於行為人，應適用新法裁判，筆者亦較贊同此見解。

陸、結語

自歐洲網路犯罪公約簽署後，該公約已成為世界各國網路犯罪立

[33] 竊盜罪為非告訴乃論之罪，刑法第三百五十八條及第三百五十九條則為告訴乃論之罪。

[34] 參見司法院(八九)廳刑一字第００八三七號函，司法周刊第九八三期第三版。

法之重要標準，我國在網路犯罪實體法部分，因本次電腦犯罪專章之補充，已大致能符合國際標準，我國相關主管機關應立即以該國際標準重新檢視網路犯罪程序法之部分，以使我國網路犯罪程序法之部分亦能臻國際水準。

司法審理網路犯罪案件時，除條文之文義解釋外，亦同時面對真實空間與虛擬空間基本價值觀之衝突與挑戰，本次修正條文之適用與解釋，仍有賴司法人之智慧與經驗累積，以釐清法律適用之界限。限於篇幅，筆者僅能簡述至此，如有未盡之處，敬請各方先進不吝賜教。